The E-Sign Act: A Federal Foundation for E-Commerce (10/00)

by Roland Brandel and Veronica McGregor

The 2nd Annual Spring Meeting
OF THE **BUSINESS LAW SECTION**
AND THE **INTELLECTUAL PROPERTY SECTION**
OF THE STATE BAR OF CALIFORNIA
APRIL 27-29, 2001, HILTON LA JOLLA, TORREY PINES

On June 30, 2000 President Clinton signed into law S.761, the "Electronic Signatures in Global and National Commerce Act" (the E-Sign Act). In doing so, the federal government put in place a cornerstone for e-commerce in the 21st century. Its passage was timely. Electronic commerce is predicted to continue its explosive growth from near zero four years ago to a volume in excess of one trillion dollars by 2002. A rapid response to alter our legal structure to accommodate the major societal changes and methods of doing business implied by e-commerce was imperative. Congress was not, however, acting alone nor even taking the lead in attempting to establish an appropriate framework for e-commerce. With the approval by the National Conference of Commissioners on Uniform State Laws (NCCUSL) of the Uniform Electronic Transactions Act (UETA), in July 1999, a number of states took immediate action to adopt UETA. Some states had adopted e-signature and related legislation even prior to the approval of UETA. This article will explore the provisions of the federal E-Sign Act and some aspects of the relationships between that Act and provisions of state legislation covering similar subjects.

Importance of the E-Sign Act Coverage Core Principles Consumer Protections Preemption Issues	Retention of Records Notarization Specific Exceptions Applicability to Federal and State Governments Conclusion

Importance of the E-Sign Act

Rather than being prescriptive or limiting, the E-Sign Act is enabling legislation. It creates a general principle of equivalency between the electronic versions of contracts, signatures, disclosures and other records and their paper-based analogs. For many industries the efficiency of electronic contracting and disclosure will reduce the cost and time for contract formation, transaction documentation and record storage.

Under the E-Sign Act, customers can get documents more rapidly and in a form that can be easily incorporated into other data files (*e.g.* a home financial management software package), or stored for later retrieval. The E-Sign Act will also enable customers to send inquiries or request documents electronically and thereby save businesses enormous amounts in personnel, printing and postage costs. For example, a single large bank making a single required disclosure (*e.g*., a monthly statement) for a single product (such as an eight million bank-card portfolio) may be able to save as much as $100 million in a single year simply by sending such disclosure electronically. Of course, that hypothetical is unrealistic in the near term because a large percentage of the customers in such a credit card portfolio may not currently have the capacity to receive electronic disclosures. Further, even some of those who do have that capacity may choose, as is their right, to continue to receive their periodic statement through the mail. Nevertheless, the E-Sign Act creates the opportunity for immense societal savings and a more efficient way to do business.

Advocates of legislation such as UETA and the E-Sign Act were critically aware of these efficiencies and the rapid implementation of technology that was placing a strain on the existing legal structures. For that reason, in 1997, NCCUSL formed a drafting committee to produce what eventually became UETA and encouraged a very rapid development of that law. At the federal level, discussions of e-signature legislation began in February of 1997 in the House. As early as July 1997, members of Congress were claiming that a federal law on the subject might be necessary because of conflicting state laws. At that point in time, over thirty states had passed or were considering some type of electronic signature laws. Although several federal bills designed to standardize electronic signature law had been previously introduced, the first bills to get serious attention were both introduced in 1999: S. 761 (the "Millennium Digital Commerce Act") on March 25, and H.R. 1714 (the "Electronic Signatures in Global and National Commerce Act") on May 6. All of these efforts had two related and important goals: to pass legislation that would facilitate e-commerce and to try to ensure uniformity with respect to the foundation principles of e-commerce functionality.

NCCUSL completed its work in only two years and approved the final version of UETA for state adoption in late July 1999. Unfortunately, the first state to act, California, passed a decidedly non-uniform version of UETA[1] almost immediately, on September 9 (signed by the Governor on September 16, 1999). The lack of adherence by California to the NCCUSL-approved version of UETA was very disturbing to the national business community, which had anticipated that UETA, as its name implied, would result in a uniform statutory basis for e-commerce throughout the country.

The California experience accelerated and altered the federal effort. By mid-November 1999, just six months after the House introduced its bill, both S. 761 and H.R. 1714 passed their respective chambers by lopsided margins—the Senate by unanimous consent and the House by a vote of 356 to 66. The two bills were in fact quite different. However, the political pressure to reconcile the differences was strong, and on June 14, 2000, the bill that emerged from the Conference Committee passed the House by a vote of 426 to 4 and the Senate by a vote of 87 to 0. President Clinton signed the bill into law on June 30. While the vast majority of the E-Sign Act became effective on October 1, 2000, the provisions pertaining to record retention are not effective until March 1, 2001.

The speed with which the bill was passed and the overwhelming congressional endorsement of the bill indicated the interest and enthusiasm of Congress in encouraging e-commerce and its desire that the principles of the E Sign Act be uniform throughout the country.

Coverage

The E-Sign Act applies to all types of transactions that occur in interstate and foreign commerce, unless specifically excepted. Arguably, with the E-Sign Act in place no state legislation on this subject was necessary (other than to cover those matters expressly excepted from the E-Sign Act). The Act contains, however, an unusual scope provision. Section 101(a), which establishes the basic rule of electronic equivalency, does so "with respect to any transaction in or affecting interstate or foreign commerce . . . ." Such language is frequently part of legislative findings to justify, constitutionally, the ability of Congress to legislate with respect to commercial endeavors.[2] Once Congress has determined, however, that particular commercial activity, as a category, either affects or is in interstate or foreign commerce, legislation does not typically segregate, in terms of coverage, particular transactions actually affecting interstate commerce from those that do not. In contrast, the E-Sign Act appears to articulate its scope on a transactional basis. It could be argued, therefore, that, with respect to the E-Sign Act, only transactions that actually affect or are in interstate or foreign commerce are, in fact, covered. As a practical matter, there is unlikely ever to be any serious issue with regard to the coverage of Internet transactions, all of which may involve interstate communications, no matter in what close geographic proximity the parties to a transaction may be.

A second coverage question is whether the E-Sign Act covers transactions that involve governmental units. The question arises because the Act covers "transactions," a defined term. UETA, from which much of the E-Sign Act was borrowed, defines transaction to encompass "business commercial, or *governmental* affairs."[3] The E-Sign Act, notably, encompasses "business, consumer or commercial affairs" (adding "consumer" and deleting "governmental").[4] This explicit language difference has caused some to conclude publicly that the E-Sign Act does not cover transactions to which governmental units are a party. Although the drafting contrast is troubling, there is ample evidence that Congress thought it was covering governmental transactions. Further, the adverse public policy consequences, for governmental units and private parties alike, of non-coverage are likely to be a powerful influence on any court faced with the issue.

Core Principles

Section 101(a) sets out the basic equivalency rule established by the E-Sign Act; it equates electronic signatures and records with their paper counterparts. Section 101(a)(1) covers documents that are retained in electronic form as well as disclosures, notices, statements and the like. Section 101(a)(2) covers electronic contract formation and provides that a contract may not be denied legal effect solely because an electronic signature or electronic record was used in its formation.

To capture the scope of the Act, two terms need to be understood. Those terms are electronic signature and digital signature. The former is a defined term in the E-Sign Act and the latter is not.

Section 106(5) defines electronic signature as "an electronic sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." "Electronic signature," therefore, is an umbrella term used to describe a category of electronic processes that may be substituted for a handwritten signature. A typical electronic signature may be as pedestrian as a typed name on an e-mail message or an activation of an "I accept" button on an e-commerce site, or as unusual as a computerized image of an actual handwritten signature. Note that the definition does not require the use of any particular authentication, encryption or identification methodology. A garden-variety electronic signature, then, assures neither the integrity (message content unaltered), authenticity (identity of the sending party), nor confidentiality of the signature or the electronic record to which it is applied. Note also that an electronic signature may be communicated orally (e.g. over the telephone), not necessarily in the form of binary bytes over the Internet or dedicated lines. Electronic signatures, are not, therefore, necessarily digital signatures. While these terms are frequently used interchangeably, digital signatures are a subcategory of electronic signatures.

The term "digital signature" has also come to have a more specialized definition, one that refers to the method of assuring message integrity. Digital signature, in this sense, refers to a specific type of electronic signature that is designed to ensure greater integrity of signed information through the use of advanced asymmetric cryptography, such as Public Key Encryption (PKE). This particular cryptography system generates and employs a secure key pair, consisting of a private key (known only to the sender) for encrypting a digital signature, and a public key (known to all possible receivers) to verify a digital signature. In a PKE transaction, the sender's message is transformed into a jumbled "hash" of characters (the "digital signature") such that only a person having the signer's public key can accurately determine whether the message received was created using the sender's private key and, therefore, whether that message has been altered from its original state. Although the recipient will be assured that the message received was sent with the sender's private key, digital signatures provide the recipient no way of knowing who actually sent the message.

Enter the certifying authorities and digital certificates. A certifying authority is a third party who will issue a digital certificate to a sender. The digital certificate verifies the identity of the sender when attached by the sender to electronic records. In some respects certifying authorities serve a notarial function. That is, a digital certificate originates from a third party who is willing to certify to an electronic record recipient that the person originating the electronic message or signing the electronic contract is who he or she purports to be. In an Internet environment, which has a high level of anonymity, devices like digital certificates and passwords may become important in situations where a recipient of an electronic signature wishes to bind the purported sender. When properly authenticated by a certifying authority, digital signatures provide a high level of security and reliability available for replacing paper signatures and records in e-commerce.

Although such technology is available and widely used, the E-Sign Act contains no mandate to provide protections with regard to message integrity, confidentiality or identity of the sender. Nevertheless, in the world of e-commerce contracting parties may wish to have varying degrees of assurance as to each of those characteristics. As none of those characteristics can be reliably achieved with a simple electronic signature, a party may choose to utilize encryption for confidentiality, a digital signature for message integrity and a digital certificate or other feature for assurance as to the identity of the author of the message.

Consumer Protections

Congress was particularly concerned that the E-Sign Act contain consumer protections for those being asked to accept electronic records in lieu of paper. Congress focused on the substitution of electronic transmittals of various mandatory consumer disclosures, notices and statements. That concern is addressed in Section 101(c)(1), which allows for required information or records to be sent electronically instead of on paper so long as the consumer has affirmatively consented to such substitution. Section 101(c) further provides for some significant disclosures regarding the conversion that must be made prior to the consumer's consent. In sum, the consumer must be informed of his or her rights to receive the records at issue in paper form, the scope of the consent sought from the consumer, the consumer's right to withdraw consent, the procedures available to the consumer to withdraw consent, how the consumer may obtain a paper copy of an electronic record, and whether any fee will be charged for such a copy. In addition, per Section 101(c)(1)(C), the consumer must be provided with a statement of the hardware and software requirements for access to and retention of the electronic records and the consumer must consent electronically in "a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used . . . ."

Recognizing the expense associated with soliciting consumer consents and the disruption that would occur if consumers already receiving electronic disclosures had that service interrupted while a consent consistent with Section 101(c) was solicited, Congress provided that the consent provisions of Section 101(c) do not apply "to a consumer who has consented prior to the effective date of this title to receive such records in electronic form as permitted by any statute, regulation, or other rule of law."[5]

If initiating hardware or software changes poses a material risk that the consumer will not be able to access or retain a record that was a subject of the consent, the sender has an ongoing duty to advise anew of any revised hardware and software requirements and to give the consumer the ability to withdraw consent without any fees for such withdrawal.

Note that although the Act considers oral electronic communication, such as instructions delivered over the telephone, to be an electronic signature in some instances, an oral communication or recording will not suffice under Section 101(c)(6) as consent to receive electronic consumer disclosures and notices.

Congress took great pains to ensure that the conversion from paper to electronics would impact the media used and nothing more. Congress expressly indicated in section 101(c)(2)(A) that "nothing in this title affects the content or timing of any disclosure . . . required to be provided . . . to any consumer . . ." and in section 101(f) that "nothing in this title affects the proximity required by any . . . rule of law with respect to any warning, notice, disclosure or other record required to be posted, displayed or publicly affixed." In section 101(g), Congress similarly and specifically protected any rules of law that require that a signature or record be "notarized, acknowledged, verified or made under oath . . . ."

While Congress clearly did not wish to impact any existing consumer protection provisions, it demonstrated some skepticism with regard to the necessity of some of the very consumer protection provisions it created in Section 101(c). For instance, Congress delegated to federal regulatory agencies the ability to "exempt without condition from the requirements relating to consent in Section 101(c) if such exemption is necessary to eliminate a substantial burden on electronic commerce and will not increase the material risk of harm to consumers."[6] In addition, Congress required in a short time frame, namely prior to June 30, 2001, the Secretary of Commerce and the Federal Trade Commission to evaluate a part of the consumer consent provisions that was viewed as particularly questionable by the business community. That is the requirement in Section 101(c)(1)(C)(ii) that requires that a consent or confirmation of a consent be given "in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used . . . ." Section 105(b) not only requests an evaluation but a suggestion of "any revisions to the provision deemed appropriate . . . ."

Preemption Issues

As noted above, beginning before the federal bill was passed by Congress, and since its passage, twenty-two states have adopted a version of UETA. Seven other states have introduced versions of UETA. Additionally, even before UETA was approved, a number of states had adopted statutory provisions dealing with the use of electronic signatures and records. The congressional goal of uniformity, however, mandated that the E-Sign Act contain a potent preemption provision. Whether the preemptive effect of the E-Sign Act will be interpreted in such a way as to provide for strong preemption and the attendant uniformity is an open question until the issues receive judicial scrutiny. In a provision entitled "Exemption to Preemption" (Section 102), Congress actually provided that in certain instances a state law might "modify, limit or supersede the provisions of Section 101."[7] One such instance is when a state has enacted UETA "as approved and recommended for enactment by NCCUSL."[8] In states like California, however, where a significantly amended version of UETA was adopted, the special rule of Section 102(A)(1) would not apply.

Even in those instances where a state adopts the uniform version of UETA, Section 3(b)(4) of UETA, which allows states to except from the scope of UETA such laws as they deem appropriate, is explicitly preempted.[9] Both the business community and Congress feared overstepping by the states in applying Section 3(b)(4) of UETA. Such overstepping would create numerous exceptions and erode the equivalency principle. That erosion would likely result in statutory confusion rather than the intended uniformity. It appears, therefore, that only state exceptions which are similar if not identical to those contained in the E-Sign Act will be construed as valid. All other exceptions should be viewed as preempted.

As a further indication of congressional distaste for exceptions to the equivalency doctrine, note that Congress required that the Secretary of Commerce report to it within three years whether even the limited exceptions created by Congress "continue to be necessary for the protection of consumers."[10]It further granted authority to federal regulatory agencies to, in prescribed circumstances, essentially override one or more of the congressionally created exceptions and thereby "extend the application of Section 101."

With regard to all other legislation on this topic a different "exemption to preemption" standard is imposed under Section 102(a)(2)(A). That provision permits a state alternative requirement only if it is "consistent" with Titles 1 and 2 and if it does not create a discriminatory requirement that specifies the application of a specific technology or technical specification.

What of a non-uniform UETA? In spite of some arguably inconsistent provisions, Congress deliberately allowed the coherent body of law created by NCCUSL to supersede or change the principles it had enacted in the E-Sign Act. Congress, therefore, clearly viewed the approved version of UETA as a reasonable alternative to the E-Sign Act. In fact, if UETA is adopted in its uniform version, there is no requirement of consistency with respect to the E-Sign Act. What is not as clear is what happens if a state adopts a non-uniform version of UETA. As the general theme of E-Sign is that all state laws must be either the approved form of UETA or completely consistent with E-Sign, perhaps the most logical reading is that any non-uniform enactment must be analyzed under Section 102(a)(2), provision by provision, for consistency with E-Sign.

Another area of uncertainty is how the courts will apply the "exemption to preemption" provision contained in Section 102(a)(2)(A). Specifically, Section 102(a)(2)(A)(i) requires that alternative procedures or requirements be "consistent" with Title I and Title II before they may "modify, limit, or supersede" the provisions of Section 101. It is conceptually difficult to imagine a legal provision that may limit or even supercede the E-Sign Act as being "consistent" with it. It is possible, however, to envision state provisions that might add requirements to those contained in Section 101 and to conclude that Congress might permit such provisions to coexist with the principles contained in Section 101. There is even some statutory support that such an interpretation might be appropriate, by contrasting 102(a)(2)(A)(i) with a provision contained in Section 104(b)(2)(B). That latter provision preempts any attempt by a federal or state regulatory agency that adopts any regulation unless it "does not add to the requirements" of Section 101. Section 102(a)(2)(A) contains no such stated provision prohibiting additional requirements.

If so interpreted, these two sections may create inconsistent rules with regard to the ability of state regulatory agencies to adopt regulations in this field with respect to electronic signature and records. A potentially more appropriate reading, however, would play down any difference between 102(a)(2)(A)(i) and 104(b)(2)(B) and instead focus on the presumed congressional goal of a uniform set of rules that facilitated rather than impeded the development of e-commerce. Hence, additional requirements that make e-commerce more difficult should be preempted.

Retention of Records

Where there is a legal requirement that records be retained in writing, being able to maintain such records electronically will likely result in enormous cost saving to U.S. businesses. The legal ability to store records electronically is contingent upon the accuracy of the record and the ability to accurately reproduce the record for later reference.[11] Records not meeting those prerequisites may not take advantage of the equivalency principle of the E-Sign Act.

Notarization

The E-Sign Act has generated major public policy debates on issues associated with notarization and acknowledgement of documents. For example, one of the essential features of a traditional notary's function has been to witness the signing in person. Serious questions arise as to how this function ought to be performed in the world of e-commerce. Congress specifically provided for electronic notarizations in the E-Sign Act, but left the questions of the appropriate requirements and information to be included in the notarization to other legal doctrine.

Specific Exceptions

Congress excepted from the coverage of the Act very few areas of human endeavor. The exceptions are set forth in Section 103. They consist of family law and probate law, most of the Uniform Commercial Code,[12] court documents and a list of notices that concern important impacts on the lives of the consuming public (*e.g.* a notice of termination of utility services or an eviction notice).

Applicability to Federal and State Governments

Congress was importuned to give flexibility to various regulatory agencies to permit them to interpret Section 101 in ways that would reflect the special circumstances they face. Congress passed provisions that preserved existing rulemaking authority, but put both state and federal regulatory agencies on an exceedingly short leash in terms of permitting interpretations that might be disruptive to the general goals of uniformity and e-commerce facilitation. Any interpretation made by a state or federal regulatory agency would be preempted unless: (1) it is consistent with Section 101; (2) it does not add to the requirements of Section 101; (3) the agency makes a special finding that such an interpretation is necessary and "will not impose unreasonable costs on the acceptance and use of electronic records;" and (4) the requirements do not favor any specific technology (a theme throughout the legislation).[13]

In a major concession not only to federal and state regulatory agencies but to self-regulatory agencies as well, Congress allowed agencies to continue to impose their own requirements with regard to filings made with such organizations. Subject to the duties of such agencies under the Government Paperwork Elimination Act,[14] the provision of Section 104(a) appears not only to permit agencies to require "specified standards or formats" but also to allow such agencies to continue to require paper filings rather than electronic filings so long as such requirements do not conflict with the Government Paperwork Elimination Act.

Conclusion

This article provides a high-level view of an Act that establishes a basic, almost universal, principle in U.S. jurisprudence. The equivalency principle for electronic signatures and records is simple in the recitation. Its universality, however, raises numerous issues, some of which surfaced during the high-speed, "Internet-time" legislative process and some of which did not. We raise some of those issues above; more are being identified every day as businesses, consumers and governmental units plunge into cyberspace and seek to make use of the equivalency principles.

---

[1] California bill S. 820 chaptered as Civil Code Title 2.5, Section 1633.1 *et seq*.

[2] U.S. Const. Art. I, § 8, clause 3.

[3] UETA § 2(16) (emphasis added).

[4] E Sign Act § 106(18).

[5] *Id.* at Section 101(c)(5).

[6] *Id.* at Section 104(d)(1).

[7] *Id.* at Section 102(a).

[8] *Id.* at Section 102(a)(1).

[9] "[A]ny exception to the scope of . . . [UETA] enacted by a state under Section 3(b)(4) of such Act shall be preempted to the extent such exception is inconsistent with this title or title II, or would not be permitted under paragraph (2)(A)(ii) of this subsection . . ."

[10] E-Sign Act Section 103(c)(1).

[11] *Id.* at Section 101(d)(e).

[12] The E-Sign Act does apply to UCC transactions in goods and leases of personal property (Articles 2, 2A).

[13] The E-Sign Act at Section 104(b)(2).

[14] The Government Paperwork Elimination Act (GPEA) was enacted October 15, 1998, and requires federal agencies to make electronic versions of their forms available online and allows individuals and businesses to use electronic signatures to file these forms electronically within five years from the date of enactment. The intent of the law is to provide a framework for reliable and secure electronic transactions with the federal government, save American individuals and companies millions of dollars and hundreds of hours currently wasted on government paperwork, and remain "technology neutral" (not inappropriately favor one industry over another).

The 2nd Annual Spring Meeting BUSINESS LAW SECTION